RECEIVED
CENTRAL FAX CENTER
JAN 18 2007

REMARKS

Applicants respectfully request reconsideration of the pending claims in light of the enclosed amendments and the following remarks. In particular, Applicants note that the specification supports the claim amendments submitted in the previous response dated January 21, 2006 as follows. The applicants have described how their media player (denoted as a "player") itself implements the disclosed content key digital rights management (CKDRM) scheme as supported on page 11, lines 14-18. On this same page at line 20, the Applicants note that this player may "embed an engine that operates with the CKDRM to provide security." Thus, for example, when Figure 4 illustrates "host 310," "engine 308," and "media 306," the engine is plainly embedded in a player – otherwise, the engine could not access the media to write or read content according the CKDRM being implemented. Note the advantages of the CDDRM illustrated in Figure 4: the host 310 (for example, a PC) has no access to the CKDRM implementation, which is controlled by the engine embedded in the player. Accordingly, the Applicants have abundant written support the amendments presented in the response of January 21, 2006.

To specifically address the location of "a section wherein the media player rather than a host, generates the random number and encrypts the session key as stated in claim 1" as noted on page 3 of the current office action, Applicants point to Figure 6 and the supporting discussion in the specification. As seen in Figure 6, the engine (element 604, which is embedded in a media player as discussed previously) includes a random number generator 618 that generates the random number used to encrypt the session key in block 620. With regard to the discussion in paragraph 206 used in the current office action to equate the host and the player, Applicants freely admit that they did disclose the possibility as stated on page 11, lines 20-21 that the player, rather than embed the engine, may be coupled to, for example, a personal computer [the host]. However, Applicants have the right to claim any embodiment disclosed and enabled by their specification – and in that regard, they can choose to merely claim the player-with-embedded-engine embodiment.

Because the Applicants have abundant written support for the amendments presented in January 21, 2006, Applicants respectfully request that the Examiner reconsider the following: Note the advantages of the media player recited in claim 20: the DRM (digital rights

management) is controlled by the media player rather than a host. This is advantageous because hackers cannot obtain access to the workings of the media player as they would for a typical host such as a PC. As claimed, the host receives encrypted content from the media player. But the host has no control over access to the content key – that access is controlled by the media player. In contrast, the Hurtado reference is a conventional "host-based" DRM scheme. In that regard, the office action of 8-18-06 states that Hurtado discloses a block configured to transmit a session key to the host in paragraphs 18, 181, 185 and 206-215. But note that these paragraphs are directed to the generation at the clearing house (element 105) of a decryption key. See, e.g., paragraph 181. Indeed, consider the end user device in Hurtado (Figure 1D). As set forth in the abstract, this end user must establish a "secure connection with an authorization authority" to decrypt desired content. As such, this is a classic host-based DRM scheme. Whatever media player the Hurtado user device contains is entirely passive: just a disk reader. It in no way generates a random number, transmits the random number to a host, etc. Instead, it is the clearing house in Hurtado that generates the decryption key. In sharp contrast, it is the media player in claim 20 that generates the random number that enables a connected host device to decrypt content it is accessing through the media player.

The Liu reference (USP 6,760,752) adds nothing further. The Liu reference is merely directed to secure transmission of data over a network (see, e.g., the abstract). Liu provides no teaching or suggestion to modify the conventional host-based DRM scheme in Hurtado into the advantageous storage-engine-based DRM provided by the storage engine of claim 20. Accordingly, claim 20 is patentable over the cited prior art.

Claim 1 is patentable for analogous reasons. The cited prior art provides no suggestion or teaching for the inventive acts of "generating a random number at the media player and encrypting the random number with a public key extracted from the certificate to form a session key and transmitting the session key to the host" and "receiving an encrypted content key from the media player and decrypting the content key using the session key to recover the content key." Given these acts, the flow of content from the media player to the host is enabled as recited by the acts of "at the media player, retrieving encrypted content from a media; transmitting the encrypted content to the host; and at the host, decrypting the encrypted content using the content key. As discussed above, the Hurtado reference is a conventional host-based scheme. There is no suggestion or teaching of a media player in Hurtado that generates a

random number and encrypts the random number with a public key to form a session key and that transmits the session key to the host. Instead, all Hurtado discloses is a user device receiving decryption information through a secure connection to a clearing house. That is host-based and thus vulnerable to hacking scheme. In contrast, all the DRM "intelligence" recited in claim 1 is retained in the media player – a user has no access to this DRM capability and thus cannot hack it. Note further that content on the media is encrypted according to a content key. Thus, the host needs the content key to gain access to the content. However, for additional security, the media player does not simply provide the content key to the host. Instead, the content key is encrypted using the secure session key. Thus, the host can only recover the content key using the secure session key. As such, the secure session key is not a content key but rather is a key to the content key.

Thus, claim 1 and its dependent claims 2, 5-14, and 16-18 are thus patentable over the Hurtado and Liu references. Claim 20 is patentable for analogous reasons as discussed previously.

Claims 1 and 20 have been amended to remove an extraneous "and." This amendment is merely to form and is not in response to the art rejections.

CONCLUSION

For the foregoing reasons, Applicants respectfully submit that the claims are in condition for allowance.

If there are any questions regarding this amendment, the Examiner is invited to call the undersigned at (949) 752-7040.

Certification of Facsimile Transmission
I hereby certify that this paper is being facsimile transmitted to the U.S. Patent and Trademark Office on the date shown below.

Jonathan Hallman — January 18, 2007
Jonathan Hallman — Date of Signature

Respectfully submitted,

Jonathan W. Hallman
Attorney for Applicants
Reg. No. 42,622
Tel.: (949) 752-7040